AO-106 (Rev: 06/09)-Application for Search Warrant

FILED

DEC 11 2024

Heidi D. Campbell, Clerk
U.S. DISTRICT COURT

UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of
Information Associated with Snapchat Account "blaineh26" that is Stored at a Premises Controlled by Snap, Inc.

Case No. 24-mj-760-JFJ

FILED UNDER SEAL

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A." This court has authority to issue this warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A).
located in the Central District of California, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §§ 1151, 1152, and 2243(a)	**Sexual Abuse of a Minor in Indian Country**
18 U.S.C. § 2422(b)	**Coercion or Enticement of a Minor**

The application is based on these facts:

See Affidavit of Jessica Jennings attached hereto.

☑ Continued on the attached sheet.

☐ Delayed notice of ___ days (give exact ending date if more than _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA Jessica Jennings, HSI
Printed name and title

Subscribed and sworn to by phone.

Date: 12/11/24

Judge's signature

City and state: Tulsa, Oklahoma

Jodi F. Jayne, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OKLAHOMA

In the Matter of the Search of Information Associated with Snapchat Account "blaineh26" that is Stored at a Premises Controlled by Snap, Inc.	**Case No. _____** **FILED UNDER SEAL**

Affidavit in Support of an Application for a Search Warrant

I, Jessica Jennings, being first duly sworn under oath, depose and state:

Introduction and Agent Background

1. I make this affidavit in support of an application for a search warrant for information associated with the Snapchat account "**blaineh26**" and that is stored at a premises owned, maintained, controlled, or operated by Snap, Inc., an electronic communications service and/or remote computing service provider headquartered at 2772 Donald Douglas Loop North in Santa Monica, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Snap, Inc. to disclose to the government information (including the content of communications) in its possession, pertaining to the subscriber or customer associated with the Snapchat account, as further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review the information to locate the items described in Section II of Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request this search warrant because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant.

3. I have been employed as a Special Agent ("SA") with Immigration and Customs Enforcement ("ICE"), Homeland Security Investigations ("HSI") since July 2022 and am currently assigned to the Office of the Resident Agent in Charge in Tulsa, Oklahoma, and am currently assigned to investigate crimes involving child exploitation. While employed by HSI, I have investigated federal criminal violations related to child exploitation and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center's (FLETC) Criminal Investigator Training Program (CITP) and the Homeland Security Investigations Special Agent Training (HSISAT) program, and everyday work relating to conducting these types of investigations.

4. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application

for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

5. Based on my training, research, experience, and the facts as set forth in this affidavit, there is probable cause to believe the identified Snapchat account contains evidence, instrumentalities, contraband, and/or fruits of violations of: 18 U.S.C. §§ 1151, 1152, and 2243(a) – Sexual Abuse of a Minor in Indian Country, and 18 U.S.C. § 2422(b), Coercion or Enticement of a Minor, associated with the Snapchat accounts described in Attachment A.

Jurisdiction

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

7. When the government obtains records pursuant to § 2703, or pursuant to a search warrant, the government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2), and (3). Additionally, the government may obtain an order precluding Snap, Inc. from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize the investigation. 18 U.S.C. § 2705(b).

Snapchat Background

8. Snapchat is a free mobile application made by Snap, Inc. and is available for download through the Apple App Store and Google Play Store. The Snapchat application is used to share information through photos, videos, and chat messages.

9. To use Snapchat, a user must download the mobile application to their mobile device and sign up using their name and date of birth. The user then selects a username and password. Snapchat then requires an email address or phone number to create an account. A user can also create a vanity name.

10. "Snaps" are photos or videos taken using the camera on an individual's mobile device through the Snapchat application, and may be shared directly with the user's friends, or in a story (explained further below), or chat.

11. A Snapchat user can add Snaps to their "story." A story is a collection of Snaps displayed in chronological order. Users can manage their privacy settings so that their story can be viewed by all users, their friends, or a custom audience. A user can also submit their Snaps to Snapchat's crowd-sourced service "Our Story," which enables their Snaps to be viewed by all users in Search and Snap Map.

12. "Memories" is Snapchat's cloud-storage service. Users can save their sent or unsent Snaps, posted Stories, and photos and videos from their phone's photo gallery in Memories. Content saved in Memories is backed up by Snapchat and may remain in Memories until deleted by the user. Users may encrypt their content in Memories

in which case the content is not accessible to Snap, Inc. and cannot be decrypted by Snap, Inc.

13. A user can type messages, send Snaps, audio notes, and video notes to friends within the Snapchat application using the Chat feature. Snapchat's servers are designed to automatically delete one-to-one chats once the recipient has opened the message and both the sender and recipient have left the chat screen, depending on the user's chat settings.

14. If a Snapchat user has device-level location services turned on and has opted into location services on the Snapchat application, Snap, Inc. will collect location data, which will vary depending on the purpose of the collection. Users have some control over the deletion of their location data in the application settings.

15. A Snapchat username is a unique identifier associated with a specific Snapchat account, and it cannot be changed by the user.

16. Basic subscriber information is collected when a user creates a new Snapchat account, alters information at a later date, or otherwise interacts with the Snapchat application. The basic subscriber information entered by a user in creating an account is maintained as long as the user has not edited the information or removed the information from the account.

17. In addition to the information provided by a user to register an account, Snap, Inc. may retain the account creation date and IP address. Further Snap, Inc. also stores a user's Timestamp and IP address of account logins and logouts.

18. For each Snapchat user, Snap, Inc. collects and retains the content and other records described above.

19. Snap, Inc. retains logs for the last 31 days of Snaps sent and received, for 24 hours of posted Stories, and for any unopened Chats or those saved by the sender or recipient. The logs contain meta-data about the Snaps, Stories, and Chats, but not the content. Snap, Inc. may be able to retrieve content of some Snaps.

20. Videos and photos sent and received as Snaps are accessible to users for only a short period of time. If a screenshot is taken of an image by the recipient, the sender is notified. Videos cannot be saved by the recipient. Because of the common belief by Snapchat users that videos and photos cannot be retained by recipients, Snapchat is often used to facilitate and document criminal acts.

21. As explained herein, information stored in connection with a Snapchat account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

22. The stored communications and files connected to Snapchat account may provide direct evidence of the offenses under investigation.

23. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Snap, Inc. can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search

for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and chat logs, documents, and photos and videos (and the data associated with the foregoing, such as location, date, and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. This geographic and timeline information may tend to either inculpate or exculpate the account owner by allowing investigators to understand the geographic and chronological context of Snapchat access, use, and events relating to the crime under investigation.

24. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

25. Other information connected to the use of Snapchat may lead to the discovery of additional evidence, the identification of co-conspirators, witnesses, and instrumentalities of the crime(s) under investigation.

26. Therefore, Snap, Inc.'s servers are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Snapchat to facilitate and communicate about the crime under investigation.

27. I requested that Snap, Inc. preserve any information for the account(s) listed in Attachment A.

Probable Cause

28. In April 2024, Special Agents from Homeland Security Investigations (HSI) Tulsa Office received information regarding a 14-year-old minor victim (MV) from Tulsa Police Department. The MV resides in Catoosa, Oklahoma, in the Northern District of Oklahoma. MV is a registered member of the Cherokee Nation Tribe. A record check was performed with the Cherokee Nation, and MV is an enrolled member of the Cherokee Nation, with some degree of Indian blood.

29. On April 10, 2024, HSI Special Agent Jennings received multiple reports from Tulsa Police Department Detective Paula Maker. One of those reports details a forensic interview of MV. The following details are contained in that report or are from my review of the forensic interview recording.

30. On March 18, 2024, MV was forensically interviewed at the Children's Advocacy Center. MV revealed that she met up with a subject she knows as "Blaine" and that he is in his thirties.

31. I received information from Tulsa Police Department Detective Maker in which Detective Maker revealed that MV identified HARRIS based off of Facebook photographs for a profile of "Blaine Harris." MV's mother additionally provided Detective Maker with information that Blaine told the MV he lives in an apartment in Sallisaw. Facebook photographs of the profile for "Blaine Harris" provided by Detective Maker appeared visually similar to the Oklahoma Driver's License photographs of Michael Blaine HARRIS.

32. Regarding her interactions with HARRIS, MV stated the following:

i. MV said that she met him on Anti, a social media application, and that "Blaine" told her he was purposely looking for minors. MV told "Blaine" she was 14 years old when he asked.

ii. MV stated "Blaine" picked her up and dropped her off in a silver small boxy car.

iii. MV stated they went to a parking lot the first time and "he fingered my vagina". MV stated "Blaine" was too paranoid to get hard and that he spoke dirty talk to her.

iv. MV stated that "Blaine" lived two hours away, close to the Arkansas border.

v. MV stated that they met three times. The other two times she met him they went to a hotel behind an O'Reilly's in Catoosa. She said they had sex and took a shower together. When they got to hotel, "he put his

penis in me." She stated that he did not use protection.

vi. MV stated that the first time at the hotel, "Blaine" tied her hands behind her back and took a picture of her naked on the bed. He used his phone to take the picture. She believed he had a Samsung phone.

vii. MV stated that she sent "Blaine" pictures/videos of herself masturbating. "Blaine" saved those pictures in his camera roll. She talked to Blaine in Anti and Snapchat.

viii. The forensic interviewer asked MV what "sex" means to her. MV said when he penetrates her vagina with his penis.

33. I received additional information from Tulsa Police Department Detective Maker. Detective Maker revealed that the hotel in question, in which MV stated that she had sex with "Blaine," would be Catoosa Inn and Suites, 40 S. 193rd Street, Room 103, Tulsa, Oklahoma 74108 and the date would be January 8, 2024.

34. On May 6, 2024, I served an administrative subpoena to Catoosa Inn and Suites for a booking by Name(s): Michael Blaine Harris, Michael Harris, Blaine Harris with Known Booking(s): 01/08/2024 for Room 103. On May 6, 2024, an employee of the hotel provided me with an invoice for Michael HARRIS on January 8, 2024 for Room 103. The invoice shows that a payment of $78.79 was paid with a Visa. There is a guest signature on the page.

35. On June 12, 2024, I received additional information from Catoosa Inn & Suites regarding the booking for Michael Harris on January 8, 2024. Catoosa Inn

and Suites provided the following information for Room 103, Day In January 8, 2024 and Day Out January 9, 2024:

i. Name: Michael Blaine Harris

ii. Address: 601 N Ash St, Sallisaw, OK 749552407, USA

iii. Phone # 580-729-0946

iv. ID Type: Driver License

v. ID #: M0XXXXXX39

vi. Issue Place: Sallisaw

36. On June 21, 2024, Homeland Security Investigation Special Agents and Task Force Officers as well as other law enforcement officers served federal Eastern District of Oklahoma search and seizure warrants for the residence, vehicle and person of Michael HARRIS. One of the items seized pursuant to the search warrants was a Samsung cell phone found on HARRIS's person. A forensic examination of that phone revealed that the Mobile Station International Subscriber Directory Number (MSISDN) of that phone is 15807290946.

37. On September 12, 2024, I was reviewing a federal search warrant return for the MV's Snapchat account that was received for another case in which the MV is a victim. Within that Snapchat search warrant, I discovered the following messages:

i. kalpows to blaineh26: "No Iâ€™m back in bed just had to go to the bathroom and Iâ€™m free this weekend" (Thu Jan 04 03:52:44 UTC 2024)

ii. kalpows to blaineh26: "513 West Denny St" (Thu Jan 04 04:09:44 UTC 2024)

iii. kalpows to blaineh26: "I want you to cum in me so badðŸ˜©" (Fri Jan 05 18:43:50 UTC 2024)

iv. kalpows to blaineh26: "Thatâ€™s good" (Sat Jan 13 17:01:14 UTC 2024)

v. blaineh26 to kalpows: "No pain either!!" (Sun Jan 21 22:53:51 UTC 2024)

38. On September 17, 2024, HSI Tulsa received the results of an administrative summons to Snap, Inc. for the subscriber information associated with "blaineh26". Within that return, under a section labeled "Account Change History" a phone number of 1-580-729-0946 is listed.

Information to be Searched and Things to be Seized

39. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Snap, Inc. Because the warrant will be served on Snap, Inc., who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

40. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by

using the warrant to require Snap, Inc. to disclose to the government digital copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

41. In conducting this review, law enforcement personnel may use various methods to locate evidence and instrumentalities of the crime(s) under investigation, including but not limited to undertaking a cursory inspection of all information within the account described in Attachment A. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, particularly including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with e-mails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account as it is impossible to know in advance all of the unique words or phrases investigative subjects will use in their communications, and consequently there are often many communications in an account that are relevant to an investigation but do not contain any searched keywords.

Conclusion

42. Based on the information above, I submit that there is probable cause to believe that there is evidence of violations of 18 U.S.C. §§ 1151, 1152, and 2243(a) – Sexual Abuse of a Minor in Indian Country, and 18 U.S.C. § 2422(b), Coercion or Enticement of a Minor, associated with the Snapchat account described in Attachment A.

43. I request to be allowed to share this affidavit and the information obtained from this search (to include copies of digital media) with any government agency, to include state and local agencies investigating or aiding in the investigation of this case or related matters, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions from this matter.

Respectfully submitted,

Jessica Jennings
Special Agent
Homeland Security Investigations

Sworn and subscribed by telephone this 11th day of ~~October~~ December of 2024.

JODI F. JAYNE
UNITED STATES MAGISTRATE JUDGE
NORTHERN DISTRICT OF OKLAHOMA

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with the following Snapchat accounts:

"blaineh26"

which are stored at the premises owned, maintained, controlled, and/or operated by Snap, Inc., a company headquartered in Santa Monica, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Snap, Inc.

To the extent that the information described in Attachment A is within the possession, custody, or control of Snap, Inc., regardless of whether such information is located within or outside the United States, and including any messages, records, files, logs, photographs, videos or other information that has been deleted but is still available to Snap, Inc., or has been confirmed preserved pursuant to a request made under 18 U.S.C. § 2703(f), Snap, Inc. is required to disclose the following information to the government for each account listed in Attachment A:

A. All stored communications and other files in Snap, Inc.'s possession (including account access information, event histories including dates and times, connection dates, times and locations, connection IP information, message content, graphics files, attachments, etc., further detailed below), whether physical, stored on electronic media, or temporarily extant on any computer or server, reflecting communications to or from the Snapchat account identified in Attachment A;

B. All subscriber information, including Snapchat username vanity names, email addresses, phone numbers, full name, physical address, and other personal identifiers;

C. All information pertaining to the creation of the account, including date and time of creation, IP address used to create the account, and all subscriber information provided at the time the account was created;

D. Timestamp and IP address of all account logins and logouts.

E. Logs of all messages and all files that have been created and Snaps sent or accessed via the Snapchat account identified in Attachment A, or that are controlled by user accounts associated with the Snapchat account;

F. The account name, vanity name, identifiers and all available subscriber information for any other Snapchat account(s) associated with the Snapchat account listed in Attachment A;

G. All content, records, connection logs, and other information relating to communications sent from or received by the Snapchat account identified in Attachment A, including but not limited to:

1. Transmitter/Sender identifiers (i.e., addresses and/or IP address);
2. Connection date and time;
3. Method of Connection (telnet, ftp, http);
4. Data transfer volume;
5. Username associated with the connection and other connection information, including the Internet Protocol address of the source of the connection;
6. Account subscriber identification records;

7. Other user accounts associated with, referenced in, or accessed by the Snapchat account identified in Attachment A;

8. Address books, contact lists and "my friends";

9. Records of files or system attributes accessed, modified, or added by the user;

10. All records and other evidence relating to the subscriber(s), customer(s), account holders(s), or other entity(ies) associated with the Snapchat account identified in Attachment A, including, without limitation, subscriber names, user names, screen names or other identities, addresses, residential addresses, business addresses, and other contact information, telephone numbers or other subscriber number or identifier number, billing records, information about the message and Snaps and all information length of service and the types of services the subscriber or customer utilized, and any other identifying information, whether such records or other evidence are in electronic or other form. Such records and other evidence include, without limitation, correspondence and other records of contact by any person or entity about the above-referenced account, the content associated with or relating to postings, communications and any other activities to or through the Snapchat account listed in Attachment A, whether or such records or other evidence are in electronic or other form;

11. All records pertaining to communications between Snap, Inc. and the user(s) of the Snapchat account identified in Attachment A regarding the user or the user's Snapchat account, including contacts with support services and records of actions taken;

12. The content of all messages and Snaps sent, received, saved, stored, or otherwise preserved.

Snap, Inc. is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, instrumentalities, contraband, and/or fruits of violations of 18 U.S.C. §§ 1151, 1152, and 2243(a) – Sexual Abuse of a Minor in Indian Country, and 18 U.S.C. § 2422(b)—Coercion or Enticement of a Minor, including, for each account or identifier listed on Attachment A:

a. Communications between the Snapchat account identified in Attachment A and others, between June 1, 2023 and present;

b. Evidence indicating the times, geographic locations, and electronic devices from which the Snapchat account listed in Attachment A was accessed and used, to determine the chronological and geographical context of the Snapchat account access, use, and events relating to the crime(s) under investigation and to the Snapchat account user, between June 1, 2023 and present;

c. Evidence indicating the Snapchat account owner's state of mind as it relates to the crime(s) under investigation;

d. The identity of the person(s) who created or used the Snapchat account identified in Attachment A, including records that help reveal the whereabouts of such person(s);

As used above, the terms "documents," and "communications," refers to all content regardless of whether it is in the form of pictures, videos, audio records, text

communications, or other medium and whether in draft or completed form and whether sent or received;

As used above, the terms "records" and "information" includes all forms of data stored by Snap, Inc., including IP addresses, toll records, and account identifying information.

Certificate of Authenticity of Domestic Records Pursuant to Federal Rules of Evidence 902(11) and 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Snap, Inc., and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Snap, Inc. The attached records consist of _____ **megabytes/gigabytes of data** associated with the Snapchat accounts.

I further state that:

a. All records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Snap, Inc., and they were made by Snap, Inc. as a regular practice; and

b. Such records were generated by snap Inc.'s electronic process or system that produces an accurate result, to wit:

1. The records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Snap, Inc. in a manner to ensure that they are true duplicates of the original records; and
2. The process or system is regularly verified by Snap, Inc., and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature